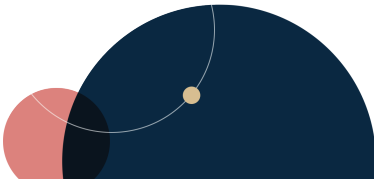
Steptoe

STEPTECHTOE | SEPTEMBER 22, 2025

A Proposed Framework for Enforcement Discretion Could Significantly Advance Deployment of AI in Highly Regulated Industries

Authors
Christian M. Auty, Tyler Evans, Jack R. Hayes, Michel Paradis, Michele Nellenbach, Elizabeth Goodwin



Overview

On September 10, 2025, Senator Ted Cruz (R-Texas) introduced legislation aimed at advancing artificial intelligence (AI) in the United States by creating a process for developers and users of AI to request modification or waiver of federal regulations that present roadblocks to deployment of new AI applications and technologies. This development could offer a powerful tool for organizations looking to deploy AI in highly regulated industries.

The proposed Strengthening Artificial intelligence Normalization and Diffusion by Oversight and eXperimentation or "SANDBOX" Act would effectively create a government-wide enforcement discretion program similar to other regulatory AI sandboxes previously proposed for specific agencies and sectors in the United States, as well as numerous other programs already implemented in Europe and Asia.

Under the Act, the Director of the Office of Science and Technology Policy would be required to establish a centralized hub to authorize temporary waivers or modifications of agency regulations to enable testing, experimentation, or temporary provision of AI products, services, business models, or production methods outside standard enforcement, licensing, and authorization regimes. This authority would also extend to sub-regulatory materials, such as agency guidance, frequently-asked-question documents, and bulletins.

Currently, the Act would not cover enforcement discretion or waivers for express statutory requirements. However, having the ability to temporarily bypass regulations and agency guidance whenever AI is involved could be a critical tool for companies that are implementing novel applications of this new technology.

Key details about the Act include the following.

1. Application Process: The Act would require that an application process be established within one year after its passage that would permit any person or the Director of the Office of Science and Technology to apply to waive or modify specific regulations or guidance for a period of 2 years. This initial 2-year period could be periodically renewed in additional increments up to a maximum of 10 years. The program would sunset 12 years after the Act is passed unless it is later renewed by Congress.

For each application, the Director would need to consult with agencies that have responsibility for the requirements that are targeted for waiver or modification. Importantly, impacted agencies would be presumed to have no objection if they do not provide input within 90 days of receiving an application from the Director or 120 days if they are granted a single available extension.

Applicants would be required to provide an analysis of the proposed benefits of the waiver or modification and explain how they outweigh potential risks. This analysis may ultimately look very similar to data protection impact assessments that are commonly required by either data privacy laws or internal government requirements regarding privacy, public engagement, or information technology.

Currently, applicants would need to deploy or plan to deploy the AI at issue through a business incorporated in the United States or with a principal place of business in the United States.

Of course, applicants would not be required to disclose trade secrets or confidential commercial or financial information as part of the application process. However, currently, the Act would not provide a blanket exemption from the Freedom of Information Act for sensitive information that is included with an application. Accordingly, traditional exemptions for proprietary or personal information would need to be applied on a case-by-case basis if a public records request is received, which could ultimately require litigation to prevent disclosure.

2. Approval and Congressional Review: Applications would be reviewed and approved by impacted agencies (or the Director on appeal from an initial agency rejection) based on a balancing of consumer benefits, enhancements to business efficiency, economic opportunities, jobs, and furthering AI innovation or development against risks to health and safety, economic damage, and unfair or deceptive trade practices.

Each year, the Director would submit a notice to Congress identifying waived or modified requirements, with corresponding recommendations for statutory amendment or repeal. The Act would include detailed rules designed to force consideration of these recommendations by Congress.

3. Appeals and Judicial Review: If an impacted agency denies an application, the Act would provide applicants with an opportunity to appeal to the Director. In addition, judicial review would be available under the Administrative Procedure Act based on agency rejections, as well as renewals and revocations of initial approvals. As a result, there would be significant room for both applicants and competitors to litigate over approvals that could end up being particularly valuable in highly regulated industries.

Revocations of initial approvals would only be expressly permitted for failure to comply with the terms of a modification or waiver, which would provide some certainty to the process and justification for efforts made in pursuing an application.

4. Approved Applicant Agreements: If approved, applicants would be required to enter into an agreement with the Director specifying each provision that is waived or modified in addition to mitigation steps each applicant will take for identified risks. In addition, each applicant would need to agree to notify the Director (and any impacted agency) within 72 hours of any incident resulting in harm to the health or safety of a consumer, economic damage, or an unfair or deceptive trade practice involving deployment of the AI at issue. Currently, this timing is tied to the occurrence of the incident and not its discovery, which could lead to technical violations of reporting requirements. Each applicant would also need to follow public reporting and notice requirements, including notices to consumers.

5. Enforcement and Related Exemptions: Approved applicants that comply with the terms of their agreements would be exempt from criminal or civil enforcement—as well as punitive agency actions like penalties, fines, or license suspensions or revocations—for regulatory provisions that have been waived or modified. However, waivers or modifications would not impact existing consumer claims.

6. Industry Examples: The Act would be especially valuable to participants in highly regulated industries. For example, the Act could be used to temporarily waive or modify regulatory requirements for financial services, as well as consumer protection rules established by the Federal Trade Commission. In addition, the Act could potentially be used to authorize waivers under export controls relating to AI hardware, software, or services, which could be critical to navigating changes in response to this rapidly evolving technology. Moreover, unique government contracting requirements, such as those applying to electronic information technology or uses of government data, could be modified or waived under the Act's authority.

Similarly, privacy and cybersecurity controls in the health care and other industries—such as "HIPAA"—could be streamlined. Employment requirements could also be targeted for applications in hiring and evaluation, especially with respect to any perceived discriminatory impacts of AI algorithms. Even antitrust guidance on sharing prices or other competitively sensitive information could be modified or waived for uses that result from training AI on this type of information.

7. Outstanding Issues and Shortfalls: Importantly, notwithstanding its potential usefulness in certain industries, the Act would not currently provide immunity from private claims. Unless changed in the drafting process, consumers could still bring private claims against approved applicants for conduct that is covered by a waiver or modification. Similarly, there would likely be an open question as to whether relator or "citizen suit" claims on behalf of the federal government or the public would be permitted. State enforcement actions would also probably still be permitted because the Act is not drafted in a way that obviously preempts state authorities that are inconsistent with a waiver or modification.

Another notable, and perhaps unintended, feature of the Act as currently drafted is that the immunities conferred by the waiver or modification would appear to apply only while an approved applicant is "in" a sandbox period. The Act currently provides that agencies may not pursue enforcement and related actions "during the period for which the waiver or modification is in effect," which raises obvious questions about whether enforcement can occur after a sandbox period expires for actions taken while the period remained in effect. The Act was likely drafted with the intent of providing indefinite protections, but that result is not expressly stated in the current text.

The Act currently only provides protection to the person for which a waiver or modification is granted. Unless approvals expressly indicate otherwise, it would not be clear whether officers, agents, employees, and third-party providers of applicants would receive the same protection. In this way, the Act is not like other federal immunity regimes that provide broad protection for all participants in certain nuclear, biodefense, and traditional defense activities. Likewise, approved applicants could have clear advantages compared to competitors engaged in very similar deployments of AI because the Act is largely drafted with protections for individual applicants in mind instead of industry-wide waivers or modifications.

Overall, the Act would establish a powerful tool for organizations that are deploying AI in highly regulated industries where federal enforcement presents a much greater risk compared to private claims or potential state violations. For example, organizations that are dealing with the complexities of deploying AI with consumer-facing or employment applications could benefit significantly from the Act. Similarly, organizations working with export-controlled or competitively sensitive information, or operating in industries like financial services or health care, could use the Act to solve novel issues that are arising from their applications of AI.

Practices

Artificial Intelligence

AI, Data & Digital

Government Affairs & Public Policy